Sociale media en surveillance

Timan, T.; Koops, E.J.

Published in:
Strafblad

Publication date:
2014

Document Version
Publisher's PDF, also known as Version of record


Dr. T. Timan en prof. dr. E.J. Koops
Timan is PostDoc-onderzoeker bij het Tilburg Institute for Law, Technology, and Society, Universiteit van Tilburg.
Koops is hoogleraar regulering van technologie aan het Tilburg Institute for Law, Technology, and Society, Universiteit van Tilburg.

44. Sociale media en surveillance: over verschuivende rollen en vervagende grenzen

In de publieke ruimte zijn toezicht en surveillance (in de Engelse betekenis van het woord) aan het veranderen door ontwikkelingen in het sociaal-technologische landschap. Denk bijvoorbeeld aan de opkomst van sociale media en alomtegenwoordige smartphones met camera's. De publieke ruimte en de privésfeer gaan steeds meer door elkaar lopen. In dit stuk kijken we naar de gevolgen van deze verschuivingen voor de organisatie van het toezicht in de publieke ruimte en voor de rechtsbescherming van de burger.

1 Inleiding[1]

1.1 Achtergrond en probleemstelling

Vooral in stedelijke omgevingen in Nederland is de publieke ruimte het object van toezicht en regulering, en in de laatste decennia is deze relatie aanzienlijk verstevigd. De publieke ruimte zegt iets over wie wij zijn als maatschappij, welke normen en waarden we willen delen en waar we voor staan. Een van die waarden is veiligheid in die publieke ruimte: eenieder moet zich in die ruimte op zijn of haar plek voelen, of in ieder geval voldoende veilig. Een technologische manier om dat doel te bereiken wordt vaak gezocht in cameratoezicht. Het idee is simpel: een lokale overheid of politie hangt camera's op in de stad en kijkt deze uit. (Omdat het een gesloten systeem is, worden dergelijk systemen vaak CCTV-camera's genoemd, naar Closed-Circuit Television.) Cameratoezicht is onderwerp van veel discussie en reflectie (zie recent bijvoorbeeld de Camover-game in Berlijn[2] en videokunst van draadloos opgevangen CCTV-beelden[3]). In de publieke en academische discussie staat CCTV vaak model voor een staat die zijn burgers in de gaten houdt. Dat komt mede omdat het een *zichtbaar* object is, met duidelijke grenzen in de publieke ruimte. Deze grenzen gelden zowel voor de fysieke aanwezigheid van camera's (zie de waarschuwingsbordjes als je een gebied binnenloopt met CCTV), als voor de verwerking van de gegevens (de beelden worden alleen opgeslagen als er voldoende reden voor is, met een meestal beperkte opslagperiode). In dat opzicht zijn het doel en de rollen van CCTV-*surveillance* helder: de politie kijkt en de burger wordt bekeken. Er zijn echter nieuwe technologische spelers in de publieke ruimte die de vorm en de rollen van toezicht doen veranderen, en daarmee implicaties hebben voor zowel de politiepraktijk als de rechtsbescherming van burgers. Een van de belangrijkste ontwikkelingen in dit opzicht is de opkomst van sociale media.
Dit brengt ons op de vraag die wij in dit artikel behandelen:

1 Dit artikel is geschreven in het kader van een door NWO gefinancierd VICI-project naar privacy in de 21ste eeuw.
2 www.theguardian.com/theguardian/shortcuts/2013/jan/25/game-destroy-cctv-cameras-berlin (alle URL's in dit artikel zijn laatst geraadpleegd op 18 augustus 2014).
3 R. van Doorn, 'Er gaat niets gebeuren', www.hollanddoc.nl/projecten/makers-van-morgen/nieuws/voorjaar-2014/er-gaat-niets-gebeuren.

wat betekent het gebruik van sociale media in *surveillance* voor de uitoefening van de politietaak en de rechtsbescherming van burgers? Om deze vraag te beantwoorden beschrijven wij hoe sociale media een rol spelen in de praktijk van *surveillance* en analyseren wij de implicaties daarvan. Voor we dat doen, geven we eerst iets meer achtergrond over sociale media en hoe daardoor *surveillance* verandert.

1.2 Sociale media en *surveillance* in de publieke ruimte

Volgens mediawetenschappers Boyd en Ellison zijn sociale media te definiëren als:

'web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site.'[4]

Waar het op neerkomt is dat er vele netwerken zijn waar gebruikers allerlei gegeven delen, van teksten en links tot foto's en filmpjes. Bekende voorbeelden zijn Twitter, Facebook en Instagram. Sommige sociale media zijn compleet open, bij de meesten is een gebruikersnaam, wachtwoord en e-mailadres nodig voor deelname aan het netwerk. De opkomst van sociale media is gepaard gegaan met een flinke stijging van het aantal en het type gegevens die gemaakt en gedeeld worden via het internet. Een paar algemene eigenschappen van sociale media zijn belangrijk om te onthouden. Sociale media zijn:

- (semi-)open: het is voor derden (zoals politie) vrij makkelijk om toegang te krijgen;
- steeds meer mobiel: ze worden meer en meer gebruikt via mobiele apparaten zoals smartphones en zijn dus 'overal en altijd' beschikbaar;
- ontworpen voor het concept van delen (*sharing*): hoe meer er gedeeld wordt, hoe beter.

Gaan we terug naar de context van *surveillance* en de rol van politie en burger, dan zien we dat het onderscheid kijker-bekekene minder scherp te maken is.
De rol van de politie in de publieke ruimte is tweeledig: handhaving van de openbare orde en opsporing van strafbare feiten. Bij 'oude' *surveillance*middelen als CCTV, dragen camera's bij aan beide rollen. Voor de opsporing kunnen ze belangrijk bewijsmateriaal leveren, maar vooral zijn camera's een welkom hulpmiddel bij het handhaven van de openbare orde als extra ogen in de publieke ruimte. Deze extra ogen dragen (idealiter) bij aan preventie, zowel om politieagenten aan te sturen in de publieke ruimte als om potentiële daders op andere gedachten te brengen. De eerste reden is vooral organisatorisch en gaat om het zo efficiënt mogelijk inzetten van blauw op straat. De tweede reden is het beoogde effect van internalisering van normen en waarden in de publieke ruimte. De redenering gaat als volgt: als burgers weten dat ze mogelijk bekeken worden via CCTV-camera's, dan zullen ze vanzelf het 'goede' doen, omdat ze weten dat er anders een kans is dat het gezien en bestraft wordt. Dit wordt het 'panoptisch effect' genoemd (naar Benthams Panopticon, zoals geïnterpreteerd door Foucault in diens theorie van, kort gezegd, *surveilllance* als zelfdisciplinering[5]). Of de camera daadwerkelijk aanstaat of uitgekeken wordt, is minder relevant: de aanwezigheid van een camera op zich is al genoeg. Het type *surveillance* dat via de CCTV-camera's plaatsvindt, is dus sterk gericht op eenweg-communicatie, met de burger als passief subject.
Het landschap op straat – de publieke ruimte – is echter de laatste tien jaar flink veranderd. Smartphones zijn alomtegenwoordig, allemaal uitgerust met een camera en meestal direct verbonden met het internet. Met één of twee klikken kan zo een straatfoto op het internet worden gedeeld. CCTV-camera's zijn daarom lang niet meer de enige camera's waarmee de publieke ruimte wordt geobserveerd: bijna elke burger heeft er ook minstens één op zak, vaak met een betere beeldkwaliteit en met snellere mogelijkheden om beelden te bewerken en te delen via een netwerk.
Dit heeft als gevolg dat de eenweg-communicatie plaats heeft gemaakt voor een mogelijke tweeweg-communicatie tussen politie en burger. De laatste heeft namelijk de mogelijkheid om terug te kijken of mee te surveilleren. In het geval van een politieoptreden of incident in de publieke ruimte is de kans welhaast groter dat het gefilmd en terug te kijken is op het internet dan dat het voorval is opgenomen door een CCTV-camera. Het fenomeen van burgers die politie of andere burgers filmen en dit delen via het internet betekent dat niet alleen elke burger potentieel een kijker wordt, maar ook dat de politie een bekekene kan worden, en dus onder potentieel toezicht staat van burgers. Wat betekent dat voor de uitoefening van de politietaak?

4 D. Boyd en N.B. Ellison, 'Social network sites: definition, history, and scholarship', *Journal of Computer-Mediated Communication* 2008, vol. 13, p. 210-230.

5 M. Foucault, *Discipline and Punish. The Birth of the Prison*, Londen: Allen Lane 1977.

2 Sociale media, openbare orde en de uitoefening van de politietaak

2.1 Digitale handhaving openbare orde

De politietaak van het handhaven van de openbare orde heeft zich uitgebreid naar het digitale domein. Niet alleen wordt er gesurveilleerd via CCTV-camera's op straat, ook digitale plekken worden in de gaten gehouden. Er wordt bijvoorbeeld gekeken naar 'trending topics' op Twitter om te kijken of er een illegaal of riskant feest gepland staat, of er wordt informatie gezocht over 'interessante personen' op sociale netwerken. Informatie die daar weliswaar door gebruikers van sociale netwerken zelf is opgezet, maar niet (per se) publiek is. Ook kunnen, via het gebruik van pseudoniemen, netwerken van mensen worden gevolgd op Facebook.[6] In het huidige politiewerk is er geen standaardprocedure of protocol voor deze vorm van *surveillance*. Er zijn grenzen aan dit digitaal rondkijken, maar die zijn nog in ontwikkeling.[7] Los van privacygrenzen is het de vraag wat dit digitaal surveilleren nu doet met de taakuitoefening van de politie. Uit een workshop gehouden met verschillende politieagenten en beleidsmakers, bleek dat digitaal surveilleren wel degelijk invloed heeft op het handhaven van de openbare orde. Zo beïnvloedt een onderzoek van sociale media bijvoorbeeld hoe de politie wordt ingezet:

'Wat je nu ziet gebeuren is dat het aantal politie-eenheden wordt ingeschat mede op basis van tweets.'
'Na de Haren-casus [project-X in Haren, TT/BJK], waren er vele oproepen binnen politiekorpsen om sociale media te monitoren en te gebruiken.'
'De politie is er echt ingedoken [sociale media, TT/BJK], zoveel is duidelijk.'
'Het bekijken van Twitter zie ik als [een vorm van] *surveillance*'.[8]

Waar het afstruinen van sociale media eerst vooral toegepast werd bij evenementen zoals voetbalwedstrijden, blijkt er een steeds grotere behoefte te bestaan om het screenen van sociale media in te bedden in de dagelijkse politiepraktijk.[9] Dat wordt ondersteund door de ontwikkeling van een infrastructuur met afgeschermde en slimme zoekfunctionaliteiten, waarbij het huidige Internet Recherche (& Onderzoek) Netwerk (iRN) wordt uitgebreid tot iColumbo, een 'intelligente, geautomatiseerde, "near" real time Internet monitoring service'.[10] Vooralsnog beperkt het onderzoek van sociale media zich vaak tot het op een afgeschermde manier 'googelen', maar op termijn zal het veredeld zoeken via platforms als iColumbo meer geïntegreerd worden in de dagelijkse politiepraktijk.

2.2 De rol van de burger

Het afstruinen van sociale media door de politie om eventuele (opkomende) incidenten op te pikken, werkt alleen als er daadwerkelijk opnames – beeld/geluid/commentaren – worden gemaakt en gedeeld. In theorie draagt al het gedeel op sociale media bij aan de vijver van informatie waar derden, waaronder de politie, in kunnen vissen. Het uploaden van foto's, filmpjes en tweets wordt echter door burgers niet per se ervaren als een bewuste vorm van meewerken aan het surveilleren van de openbare ruimte. Burgers dragen meestal onbewust bij aan het surveillanceapparaat, door bijvoorbeeld een leuk filmpje van een avond te delen, of door over een voorval te tweeten. Dit wordt ook wel 'participatieve surveillance' genoemd.[11] Het doel van dit delen ligt dan voor de burger niet primair bij *surveillance*, hun gegevens kunnen daar wel voor worden gebruikt. Uit een aantal interviews gehouden met uitgaanspubliek in Rotterdam kwamen de volgende punten naar voren over het maken van beelden:

'Nou, ja, ik maak wel foto's of filmpjes tijdens dode momenten.'
'Ik ben niet het type dat meteen haar telefoon grijpt en een filmpje maakt als er iets aan de hand is.'
'Meestal maak ik foto's van onverwachte momenten of gebeurtenissen; dat vind ik leuk om te doen.'

En over het delen ervan:

'Ja, degenen die we leuk vinden eindigen op Facebook of Hyves.'
'Ik schaam me niet echt ergens voor, dus… in die zin… Er zijn altijd mensen die willen voorkomen dat sommige zaken

6 Dat blijkt vrij makkelijk te zijn: zie www.danah.org/papers/FacebookPrivacyTrainwreck.pdf.
7 Vgl. B.J. Koops, 'Politieonderzoek in open bronnen op internet. Strafvorderlijke aspecten', *Tijdschrift voor veiligheid* 2012, p. 30-46; J.J. Oerlemans en B.J. Koops, 'Surveilleren en opsporen in een internetomgeving', *Justitiële verkenningen* 2012, nr. 5, p. 35-49.
8 Deze citaten komen uit een workshop met verschillende politieagenten, beleidsmakers en technici die te maken hebben met surveillance in Rotterdam en Utrecht. Zie ook T. Timan, *Changing Landscapes of Surveillance* (diss. Twente), 2013.
9 Vgl. D. Trottier, *Social Media as Surveillance. Rethinking Visibility in a Converging World*, Farnham: Ashgate 2012.
10 Deelprojectvoorstel 'iColumbo', geciteerd in Oerlemans en Koops 2012, p. 35. Zie ook B.J. Koops e.a., *Juridische scan openbrononderzoek. Een analyse op hoofdlijnen van de juridische aspecten van de iRN/iColumbo-infrastructuur en HDIeF-tools*, Tilburg/Delft: TILT/TNO 2012.
11 Zie A. Albrechtslund, 'Online Social Networking as Participatory Surveillance', *First Monday* 2008, nr. 3, firstmonday.org/ojs/index.php/fm/article/viewArticle/2142.

op Facebook komen. Dat geldt dus niet voor mij.'
'Oh daar ben ik echt slecht in, ik zou niet weten hoe ik een filmpje zou moeten uploaden.'[12]
Uit deze reacties op zowel het maken als het delen van gegevens kunnen we zien dat er een diffuse gebruikerspraktijk bestaat: niet iedereen maakt en deelt beelden, en er zijn uiteenlopende redenen om dit wel of niet te doen. De technologie en het gebruik van sociale media verschilt daarbij wezenlijk van die van CCTV, maar ze komen uiteindelijk wel samen omdat ze allebei een belangrijk vormend onderdeel zijn van surveillance in de publieke ruimte.
Niet alle opnames in de publieke ruimte worden voor de lol of min of meer toevallig gemaakt: het komt ook voor dat burgers bewust een politieoptreden in de publieke ruimte filmen.[13] Deze gevallen van 'counter-surveillance' of 'inverse surveillance'[14] illustreren een verschuiving van rollen, waarbij de machtsbalans tussen politie en burger enigszins verandert. Vanuit de politie wordt er verschillend gereageerd op de nieuwe actief-surveillerende burger. Uit interviews gehouden met politiemensen, kwamen de volgende punten naar voren:

'… sommige collega's zijn zich er wel van bewust en die vinden het lastig om ermee om te gaan. Je zult je erbij neer moeten leggen dat het de tijd is en dat het veel vaker zal gaan gebeuren. Iedereen heeft een mobiele telefoon en natuurlijk worden er films gemaakt… ik maak me er niet zo druk om. En wij proberen op straat altijd correct te zijn, dus ja dat levert over het algemeen wel correcte beelden op. Natuurlijk heb je wel eens een uitschieter.'
'Er was erg veel heisa bij de introductie van de bodycamera, maar mensen hebben tegenwoordig hun eigen camera en die gebruiken ze ook!'[15]

Er wordt hier gerefereerd aan het feit dat het een publieke taak betreft en als zodanig maakt het volgens de geïnterviewde niet uit of iets wordt opgenomen of niet. Toch heerst er ook twijfel bij politieagenten, vooral over hoe op te treden als er inderdaad bewust een ingreep of optreden wordt gefilmd.[16] Naarmate het besef groeit dat de aanwezigheid van burgers met smartphones steeds meer een gegeven wordt in de publieke ruimte, stelt de nieuwe realiteit zowel de burger als de politie voor nieuwe vragen omtrent de grenzen en rol van de publieke ruimte.

2.3 Implicaties

Door de komst van sociale media en de smartphone is het delen van informatie steeds makkelijker geworden. Hieraan kleven ook nadelen: het wordt ook makkelijker voor derden om toegang te krijgen tot de informatie. In de context van *surveillance* in de publieke ruimte zien we dat burgers nog steeds (meestal onbewust) leverancier zijn van informatie voor opsporing. Deze rol verschilt substantieel van de bekendere vorm van *surveillance*, cameratoezicht, door schaal (massadata) en gemak. De uitoefening van de politietaak krijgt meer het karakter van een sleepnet dan voorheen: waar er via CCTV op het moment zelf en in een beperkte, afgebakende ruimte meegekeken kan worden en achteraf maar beperkt kan worden teruggekeken, biedt surveillance van sociale media de mogelijkheid om veel meer data geautomatiseerd, en daarmee ook zonder vooropgesteld of al te specifiek doel, te verzamelen en te verwerken, van een veel grotere groep burgers dan bij CCTV in beeld komt. Dit past in de tendens van een preventiecultuur en risicosamenleving, waarbij de burger in de publieke ruimte een ander karakter krijgt in termen van object van politieonderzoek: in plaats van een toevallige passant die op sommige plaatsen in beeld komt, wordt de burger langzamerhand een structureel potentieel risico-object.
Een van de gevolgen is dat de rol van burgers aan het verschuiven is. Aan de ene kant wordt meer nadruk gelegd op burgerparticipatie bij de veiligheid in de publieke ruimte (bijvoorbeeld via oproepen om beelden te maken van incidenten en die te delen met de politie); aan de andere kant wordt diezelfde burger meer via sociale media in de gaten gehouden als een potentieel risico. Ook de rol van de politie verschuift, nu zij gebruik kan maken van sociale media. Een paar voorbeelden uit interviews:

'Dat je nu iedereen kunt volgen en dat je makkelijk toegang hebt tot informatie… dat maakt surveillance gevoeliger.'
'Het imago van de politie is tot nu toe geloofwaardig. Die positie raak je kwijt als je al je activiteiten gaat delen op Twitter.'
'Facebook, Twitter, deze diensten kun je gebruiken om

12 Citaten uit interviews gehouden met verschillende bezoekers van uitgaansgebieden in Rotterdam in 2012. Zie ook T. Timan en N.E.J. Oudshoorn, 'Mobile Cameras as New Technologies of Surveillance? How Citizens Experience the Use of Mobile Cameras in Public Nightscapes', *Surveillance & Society* 2012, p. 167-181.
13 Zie bijv. www.huffingtonpost.com/clay-calvert/filming-police-in-public-_b_5424621.html of een bekende casus in Nederland: www.trouw.nl/tr/nl/4492/Nederland/article/detail/3274336/2012/06/20/Ombudsman-geschokt-door-schopincident-agente.dhtml.
14 S. Mann, 'Sousveillance: Inverse Surveillance in Multimedia Imaging', in *Proceedings of the 12th Annual ACM International Conference on Multimedia* 2004, p. 620-627.
15 Citaten uit interviews gehouden met politieagenten en beleidsmakers te Rotterdam in 2012. Zie ook Timan 2013.
16 Zie bijv. deze reactie op het filmen van de politie door burgers: boingboing.net/2011/12/18/london-cops-apologise-to-young.html.

burgers te monitoren, maar ook om ze te informeren. Maar de gebruiker/burger kan zelf ook zenden en ontvangen. Het werkt dus twee kanten op.'[17]
De politie twijfelt en is verdeeld over hoe sociale media te gebruiken, deels vanwege onduidelijke grenzen en onzekerheid over de gevolgen voor de uitoefening van de politietaak, en deels ook uit angst dat burgers 'terugkijken'. In de huidige praktijk bestaan ook twijfels over de toegevoegde waarde van sociale media op het daadwerkelijk politiewerk.
De onzekerheid over de gevolgen van verschuivende rollen door een veranderende inzet van technologie is voorstelbaar. Technologie is niet neutraal, maar vormt samen met de gebruiker een nieuwe combinatie met unieke en vaak onvoorspelbare eigenschappen. De burger met smartphone heeft andere mogelijkheden dan een burger zonder smartphone, en

Smartphones zijn het nieuwe DNA

het verschil ligt in de combinatie van technologie en mens.[18] Daarnaast wordt technologie nooit uniform ingezet; binnen elke context ontstaat een eigen, unieke situatie. Niet alle beelden gemaakt met smartphones worden gedeeld en niet alle socialemediaberichten worden gelezen of zijn bruikbaar. De publieke ruimte is een coproductie van technologie, maatschappelijke omgangsvormen en waarden, en nu binnen die ruimte verschuivingen plaatsvinden, is nog niet goed te overzien hoe het nieuwe landschap van *surveillance* in de publieke ruimte eruit komt te zien. Dat ook de waarden in dit landschap zullen verschuiven, weten we uit de techniekssociologie en techniekfilosofie: normen en waarden, ook in de publieke ruimte, worden gemedieerd door technologie;[19] hoe ze aan het veranderen zijn, is moeilijker te zeggen. De komende jaren zullen leren wat wel en niet gepast is in het maken van beelden in de publieke ruimte, zowel door burgers als door politie,[20] in het delen van die beelden met 'vrienden' of met de hele wereld, en in de vrijheid om gebruik te maken van via het internet gedeelde of openbaar gemaakte gegevens als die niet direct bedoeld zijn voor surveillance in de publieke ruimte, maar daar wel voor kunnen worden benut. Hierbij is de uitdaging voor wetenschappers, beleidsmakers en technici om actief deel te nemen in de ontwikkeling en implementatie van nieuwe technologieën, om zo goed mogelijk te anticiperen op ongewenste gevolgen en waar mogelijk te sturen richting maatschappelijk aanvaardbare toepassingen.[21]

3 Smartphones, de publieke ruimte en rechtsbescherming

Naast het naspeuren van sociale media bij de dagelijkse handhaving van de openbare orde, komt de politie sociale media ook tegen bij opsporingsonderzoeken. In het kader van een opsporingsonderzoek is het logisch om te kijken wat er over een slachtoffer, verdachte of 'interessante personen' te vinden is in open bronnen; het kan daarbij interessant zijn om ook in besloten profielen te kijken, door onder pseudoniem in een netwerk contact te leggen met de te onderzoeken persoon. Hoewel de politie wel incidenteel en kort mag rondkijken in sociale media op basis van artikel 3 Politiewet 2012, gaat openbrononderzoek (en zeker het aanmaken van een pseudoniem profiel) al snel over in een meer dan geringe inbreuk op de privacy, zodat de grondslag van een opsporingsbevoegdheid nodig is, bijvoorbeeld een bevel stelselmatige observatie. Daarover is al het nodige geschreven.[22] Hier willen we ingaan op een ander aspect van het onderzoek van sociale media.

De politie kan bij aanhouding voorwerpen in beslag nemen die de verdachte bij zich draagt (art. 95 lid 1 Sv), bijvoorbeeld om te voorkomen dat bewijsmateriaal wordt gemanipuleerd of vernietigd. De meeste verdachten zullen tegenwoordig een smartphone hebben, waarin relevante bewijsinformatie kan staan (bijvoorbeeld over contacten of plannen). Voor de politie is het bijzonder interessant een smartphone in beslag te nemen en uit te lezen: er staan contacten, e-mailadressen, foto's, filmpjes, wachtwoorden, agenda's in, maar ook metadata zoals locaties, laatst gebruikte applicaties, belgeschiedenis, berichtengeschiedenis en wanneer en hoe vaak de telefoon is gebruikt.[23] Veel van deze informatietypen hebben te maken met het gebruik van sociale media. Smartphones zijn het nieuwe DNA.[24] Hoewel het in beslag nemen en uitlezen van een smartphone geen

17 Citaten uit interviews gehouden met politieagenten en beleidsmakers te Rotterdam in 2012. Zie ook Timan 2013.
18 Vgl. W.E. Bijker en J. Law, *Shaping Technology/Building Society: Studies in Sociotechnical Change,* Cambridge, MA: MIT Press 1992.
19 Vgl. P.P.C. Verbeek, 'Materializing Morality: Design Ethics and Technological Mediation', *Science, Technology, & Human Values* 2006, p. 361-380 of recent S. Dorrestijn, *The Design of Our Own Lives: Technical Mediation and Subjectivation after Foucault* (diss. Twente), 2012.
20 Die gebruik kan maken van draagbare bodycams; zie Timan 2013, hoofdstuk 5.
21 Binnen de context van privacy- en technologieontwikkeling gebeurt dit al enigszins via Privacy Impact Assessments. Zie ook D. Wright en P. De Hert (red.), *Privacy Impact Assessment*, Dordrecht: Springer 2012.
22 Vgl. Koops 2012; Oerlemans en Koops 2012.
23 Dit zijn voorbeelden uit een lange lijst die een politiefunctionaris noemde bij een presentatie over de praktijk van cybercrimebestrijding, tijdens een studiedag Cybercrime op 14 november 2013.
24 Ibid.

doel op zich mag zijn bij aanhouding, levert het een aantrekkelijke bijvangst op. Dat kon vroeger natuurlijk ook het geval zijn met fysieke objecten die bij aanhouding werden aangetroffen, zoals agenda's, adresboekjes en dagboeken. Maar dat waren relatief zeldzame vondsten, en bovenal meestal van een andere orde dan een smartphone. Anders dan de papieren gegevensdragers die iemand voorheen bij zich kon hebben, bevat een smartphone een tamelijk volledige blauwdruk van iemands persoonlijk leven.

Op dit punt zien we dat de publieke en de private ruimte door elkaar gaan lopen. Vroeger liet men het grootste deel van het privéleven achter in de woning (alle foto's, boeken, muziek, brieven en intieme geschriften). Tegenwoordig dragen veel mensen hun halve privéleven met zich mee in de smartphone of tablet-pc; ook wordt informatie die vroeger thuis fysiek werd bewaard, nu steeds vaker opgeslagen in de cloud, en daarmee permanent toegankelijk. De privésfeer, waaronder alle informatie die mensen in besloten sociale-medianetwerken met elkaar delen, wordt zodoende toegankelijk vanuit de publieke ruimte, wanneer de politie bij een aanhouding op straat een smartphone in beslag kan nemen en uitlezen. De fysieke bevoegdheden in de publieke ruimte – aanhouding, inbeslagneming – krijgen nu ook een digitale component, maar dat is niet simpelweg oude wijn in nieuwe zakken. Met de digitalisering en mobilisering van informatie krijgt de uitoefening van klassieke bevoegdheden in de publieke ruimte een nieuwe dynamiek.
Dat dit gevolgen heeft voor de rechtsbescherming van burgers, moge duidelijk zijn. Veel van de informatie die via een in beslag genomen smartphone beschikbaar komt, was voorheen alleen te achterhalen via een doorzoeking in de woning of via het onderscheppen van telecommunicatie: zware bevoegdheden die aan een rechterlijke machtiging zijn onderworpen. Het valt moeilijk vol te houden dat informatie in een smartphone 'bijvangst' is bij aanhouding, nu het merendeel van Nederland een smartphone op zak heeft. Bovendien, zo blijkt uit een recente uitspraak van het Amerikaanse Hooggerechtshof, gaat het onderzoeken van een smartphone in zekere zin nog verder dan een huiszoeking.

In *Riley v. California*[25] beantwoordde het Hooggerechtshof de vraag of de politie bij een verkeerscontrole, waarbij vuurwapens in de auto werden aangetroffen, een smartphone van de verdachte mocht onderzoeken zonder rechterlijke machtiging (*warrant*). Hoewel staande jurisprudentie het toestaat om bij een arrestatie zonder *warrant* objecten die verdachte bij zich draagt in beslag te nemen en te onderzoeken, teneinde bewijsmateriaal veilig te stellen of de veiligheid van de politie te waarborgen, gaf het Hof in niet mis te verstane bewoordingen aan dat een smartphone niet te vergelijken is met de oude vormen van een 'search incident to arrest' waarop de jurisprudentie was gebaseerd.

Het valt moeilijk vol te houden dat informatie in een smartphone 'bijvangst' is bij aanhouding, nu het merendeel van Nederland een smartphone op zak heeft

'[P]hones are based on technology nearly inconceivable just a few decades ago, when *Chimel* and *Robinson* were decided. (…) A search of the information on a cell phone bears little resemblance to the type of brief physical search considered in *Robinson*. (…) The United States asserts that a search of all data stored on a cell phone is "materially indistinguishable" from searches of these sorts of physical items. (…)That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. (…) In 1926, Learned Hand observed (…) that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." (…) If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form. (…) With all they contain and all they may reveal, they hold for many Americans "the privacies of life"'.[26]

Deze uitvoerige citaten uit de uitspraak onderstrepen hoezeer de privésfeer nu in de publieke ruimte is doorgedrongen. In de VS is aldus inmiddels onderkend dat de rechtsbescherming van burgers moet worden aangepast. In Nederland moet dit besef nog doordringen. De op de fysieke werkelijkheid geënte wetgeving, gebaseerd op een veronderstelling dat in de publieke ruimte de privésfeer maar beperkt aanwezig is, raakt achterhaald door de verschuivingen in het huidige technologische landschap. Evenals de Wet BOB, met een op

25 *Riley v. California*, 573 U.S. ___ (2014), te vinden op www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf.

26 Ibid.

fysieke observatie geënte regeling van stelselmatige observatie die niet goed toepasbaar is op stelselmatige observatie van sociale media,[27] zijn ook de klassieke opsporingsbevoegdheden die in de publieke ruimte kunnen worden ingezet, aan herijking toe.

4 Conclusie

Door de komst van sociale media vinden er verschuivingen plaats in de context van surveillance in de publieke ruimte. Het begrip *surveillance* wordt vaak geassocieerd met de aanwezigheid van CCTV-camera's en *big brother*, waar de politie de kijker is en de burger de bekekene. De komst van sociale media heeft een nieuwe, digitale dimensie toegevoegd aan *surveillance*, waarbij de rollen van kijker-bekekene niet meer zo scherp te onderscheiden zijn. Met het veranderen van deze rollen verandert ook de notie van publieke en private ruimte. Immers, in de publieke ruimte kon men voorheen als burger weten, of redelijkerwijs verwachten, waar de grenzen van privacy lagen, door zichtbare CCTV-camera's met waarschuwingsbordjes. Maar als burgers zelf opnames gaan maken in de publieke ruimte van de politie, heeft de politie dan het recht om hun mobiel om die reden te doorzoeken of zelfs de beelden te verwijderen? Of als iemand op straat gefilmd wordt door derden, kan zij daar dan bezwaar tegen maken, en zo ja, op welke grondslag? En wat als deze opnames (vaak beeld en geluid) op het internet terecht komen, hoe zijn de rechten van burgers dan beschermd? De privésfeer en de publieke ruimte beginnen zich hier te mengen. Om hier adequaat mee om te gaan, groeit de noodzaak van nieuwe vormen van rechtsbescherming.

De mobiliteit van de private ruimte maakt ook dat we onszelf 'altijd bij ons' hebben en daardoor mogelijk steeds minder aandacht hebben voor onze rol als publieke burger. We zijn immers niet duidelijk in de publieke ruimte, maar vaak in een 'privébubbel' in de publieke ruimte. In plaats van het panoptische effect (dat we ons beter gedragen omdat we mogelijk bekeken worden via CCTV) – lijken we nu steeds meer naar onszelf te kijken via sociale media. We zijn in die zin misschien minder gevoelig geworden voor het publieke oog dat kijkt en meer voor het private oog van onze vrienden op sociale media (waartoe in het geval van filmpjes van incidenten opsturen dan ook de politie behoort). Door actief bezig te zijn met het bijdragen aan sociale media, voeden we mogelijk surveillerende partijen met informatie. Het meedragen van een privébubbel op straat heeft in die zin een tegengesteld effect aan *participatory surveillance:* we delen meer met, maar voelen ons misschien minder verantwoordelijk voor het publieke domein.

Vaak worden technologische vernieuwingen gezien als een simpel nieuw hebbeding of gewoon een extra bron van informatie. We moeten echter niet vergeten dat de normen en waarden in de publieke ruimte geschapen worden door de combinatie van mens en techniek. Doordat we straatverlichting hebben, bijvoorbeeld, wordt de publieke ruimte 's avonds een leefbare en bruikbare ruimte. In het geval van *surveillance* hebben de CCTV-camera's ook hun invloed gehad op hoe we denken over de publieke ruimte en noties van privacy. Het surveilleren van sociale media wordt langzamerhand standaardpraktijk – vaak met het argument omdat het er is en omdat het kan. We moeten waken voor dit soort naïeve standpunten over de rol en invloed van technologie. Het is belangrijk om bij nieuwe vormen van *surveillance* die een bepaalde technologie mogelijk maakt, na te gaan hoe en op welke manier deze onze publieke ruimte kan beïnvloeden en of dat wenselijk is. Ook is meer actieve betrokkenheid belangrijk bij de ontwikkeling en toepassing van privacy- en surveillance-gerelateerde technologie, van zowel beleidsmakers en ontwikkelaars als wetgevers en eindgebruikers.

Technologie verandert de maatschappij, maar de maatschappij beïnvloedt ook technologiegebruik. Nieuwe technologie zoals sociale media leiden, zoals we in dit artikel hebben betoogd, tot verschuivingen in rollen en rolpatronen, vaak op onvoorspelbare manieren. Dit maakt het moeilijk voor de wetgever om grenzen te stellen: welk ankerpunt kiezen we? In elk geval is het wel duidelijk dat de wetgever ergens grenzen moet stellen, en dat het klassieke onderscheid tussen een publieke ruimte waar de politie surveilleert en de burger bekeken wordt, en een private ruimte waar de burger zijn privéleven leeft en de politie in principe niet binnenkijkt, niet meer goed werkt. De opkomst van sociale media en mobiele apparaten leiden tot een verknoping van de publieke en private sfeer. Dat betekent dat we moeten nadenken over hoe toezicht in (wat voorheen werd aangeduid als) de publieke ruimte wordt georganiseerd en gereguleerd, en hoe de rechtsbescherming in (wat we nu beter kunnen noemen) de publiek-private ruimte moet worden vormgegeven.

27 Oerlemans en Koops 2012.